Executive Summary

Fault Management Services for Reliable, Available and Serviceable Systems (SRASS)

Checkpoint Restart

PNUM 12A

Background: The IEEE Portable Operating System Interface (POSIX) SRASS working group is in the process of developing an open standard for fault management and serviceability applications. The goal of the SRASS Working Group is to support fault tolerant systems, serviceable systems, reliable systems, and available systems in a portable way. The key objective allows this work to be used for general applications, such as distributed, parallel, database, transaction systems and safety related systems. These draft specifications are currently cited in the DOD Joint Technical Architecture Document under emerging operating systems standards.

Scope: The SRASS Working Group (IEEE P1003.1h) and Checkpoint Restart (IEEE P1003.1m) is defining Application Program Interfaces (APIs) for event logging, core dump control, shutdown/reboot, configuration space management, and checkpoint Restart.

The objective of the logging APIs allows an application to log application-specific events and system events to a system log and for the subsequent processing of those events. Fault management applications can use this API to register for notification of events that enter the system log. Events of interest may be those that exceed some limit, a notification can have a severity associated with it etc. A notification can provide a way to react proactively and initiate steps to prevent a system failure later. Below is a summary of the key objectives these standards will satisfy. They are: 1) the event and error logging and notification API enables proactive response and fault prevention; 2) the single core dump control API enables an application to specify the file path location if a process terminates with a core dump file; 3) the shutdown/reboot API allows services to perform a fast shut down, graceful shutdown and optional features such as rebooting with optional scripts; 4) the corrective action services such as reconfiguration is included in the draft standard to keep the system operational. The configuration space management API is intended to provide a portable method of traversing the configuration space, and for manipulating the data content of nodes in that configuration space; and 5) Checkpoint Restart is a separate draft POSIX standard. It allows an application to save the entire state of the machine, the Operating System and the applications activities so if something goes wrong, the current state can be brought on line quickly.

These efforts will generate a functional requirements specification, as part of the Virtual JTA efforts, for using the JTA for the 21st century service combatant (SC21) ship.

Project Goal and Industry Support: Commitments from IBM, Sequoia, Defense Research Agency (DRA) in the United Kingdom and Clarion are members of the working group. The DRA is using the Army's RTEMS operating system to add the SRASS APIs and test their Avionics applications. Raytheon-TI, Hewlett Packard, and Honeywell have expressed an interest in the SRASS draft. The goal is to complete the JTA draft POSIX standards in time for industry to implement the services. The final product will allow DOD to procure open industry products based on the IEEE fault management and checkpoint restart standards. The Naval Surface Warfare Center - Dahlgren chairs the POSIX (SRASS) and Checkpoint Restart Standards Working Groups, supports ballot coordination for both groups, and secretary position.